

**UNITED STATES DISTRICT COURT  
DISTRICT OF NEW HAMPSHIRE**

**UNITED STATES OF AMERICA**

**v.**

**HIEU MINH NGO**

---

)  
)  
)  
)  
)  
)

**1:12-cr-144-PB**

**1:14-cr-081-PB**

**GOVERNMENT’S SUPPLEMENTAL  
CONSOLIDATED SENTENCING MEMORANDUM**

**OVERVIEW**

The Government submits this Supplemental Sentencing Memorandum for the upcoming consolidated sentencing of Hieu Minh Ngo, who was the ringleader of a massive, multi-year international computer hacking and fraud scheme involving the theft and trafficking of enormous volumes of highly sensitive personally identifiable information (“PII”). Ngo’s relentless crime spree began in 2010 and ended only when, in February 2013, USSS agents successfully lured him from his home country of Vietnam to the United States and arrested him upon his arrival at the airport. Ultimately, Ngo permanently imperiled the financial security of hundreds of thousands, and more likely millions, of U.S. citizens, and he caused a staggering guideline loss of \$65-\$100 million.

As set forth below, and in the Government’s initial Sentencing Memorandum, in light of the anticipated USSG range of 292-365 months<sup>1</sup>, the Government’s 5K motion, and the 3553 factors such as the seriousness of Ngo’s crimes, Ngo’s personal background, the profound need to protect the public from further harm, as well as to provide adequate specific deterrence to Ngo and general deterrence to other hackers, the Government urges the Court to sentence Ngo to 15

---

<sup>1</sup> The parties have filed a Joint Recommendation regarding the guideline calculation which, if accepted by the Court, will result in a sentencing guideline range of 292-365 months.

years in prison. Moreover, a 15-year sentence would be in line with other sentences meted out in this district and in other courts around the country that involved related or similar conduct.

Because the Government's prior submissions and its 5K motion lay out its position regarding the USSG Guideline's calculation<sup>2</sup> and Ngo's substantial assistance, this supplemental memo will focus primarily on the 3553 factors at play in determining an appropriate sentence for Ngo.

# **1. Nature and Scope of Ngo's Criminal Conduct and Seriousness of Offense**

As set forth in the two Pre-Sentence Investigation Reports ("PSIs") and the two indictments to which Ngo has pleaded guilty, Ngo, operating from his home base in Vietnam, was the mastermind of a widespread, international scheme that targeted and hacked into U.S. businesses and then stole a massive amount of U.S. citizens' sensitive PII. He then generated significant profits by using his black market websites to sell the stolen PII to his criminal associates, so that his buyers could in turn use the stolen PII to commit various types of fraud. These included filing fraudulent tax returns and opening lines of credit and payment card accounts in victims' names. Significantly, some of the PII that Ngo sold was an extremely robust variety of PII (which are called "fullz" or "full infos" in the cybercrime world). These "fullz" included not only the victim's name, date of birth, and social security number, but also included a vast array of other highly sensitive financial and personal information, such as the victim's email accounts and passwords, bank account numbers, and bank routing information.

In addition to hacking U.S. business' computers and stealing PII from them, Ngo also devised and successfully executed an elaborate fraud scheme so that he could gain access (and then re-sell that access to his criminal associates) to U.S. databases containing approximately

---

<sup>2</sup> In its prior submission the Government argued for a guideline loss of \$145 million but the parties have reached an agreement which, if accepted by the Court, will result in a guideline loss between \$65 and \$100 million. This will reduce the number of levels added for loss from 26 to 24, the total offense level from 42 to 40, and the advisory guideline range from 360-780 months to 292-365 months.

200 million people's PII. On multiple occasions, Ngo posed as the owner of a legitimate private investigation company so that he could trick U.S. data brokers into selling him access to their vast PII databases. In his "whack-a-mole" fraud scheme, Ngo invented, and then re-invented, himself and approached several different U.S. data brokers to sell him access to their PII. For example, after Ngo lost access to the PII database he hacked into at Microbilt (which forms the basis of the New Jersey charges), he then posed as "Jason Low" supposedly from a bogus Singapore-based private investigation company called "SG Investigators" to gain access to another U.S. PII database. When that data broker eventually closed "Low's" account (which it did after USSS agents advised it of Ngo's activities) and Ngo needed to find a third U.S. database of PII, Ngo re-invented himself yet again, this time as the owner of yet another bogus private investigator firm, an Illinois-based company called American Investigators. At the time of Ngo's eventual arrest, he was in the process of re-inventing himself once more and approaching (what he believed to be) yet another data broker. Unfortunately for Ngo, this data broker was in fact a cooperating witness working with the USSS in the investigation.

In order to try to convince the data brokers that he was legitimate, Ngo doctored up a phony Private Investigators' license and obtained a phony driver's license. Ngo also hacked into and took over the e-mail accounts of innocent individuals and then sent e-mail messages to others, posing as those individuals whose identity he had just co-opted, to convince them to do business with Ngo. He also tried to hide his identity and nationality by setting up bank accounts with third party "go-betweens" who were located in other countries.

Once Ngo successfully gained access to these vast U.S. databases of PII, he generated enormous profits for himself by re-selling that access to his more than 1,300 criminal associates. He did this by setting up his own websites and then charging his criminal buyers money to

perform “queries” on the databases. Conservatively estimated, Ngo’s criminal buyers performed three million queries into those databases and retrieved untold millions of additional U.S. citizens’ PII. For his criminal efforts, Ngo was paid \$1.75 million through Liberty Reserve payments from his bad actor clients around the globe.

Ultimately, as the Government pointed out in its initial submission, Ngo wreaked havoc on the financial wellbeing of at least hundreds of thousands, and more likely millions, of American citizens. Unlike one’s payment card data, which, when stolen, can be closed, one’s PII, when stolen, can never be “clawed back.” Ngo has irrevocably endangered almost two hundred thousand, and more likely millions more, Americans’ PII. That highly sensitive PII is now in the hands of criminals who can lay in wait for weeks, months, or years before they wreak havoc on the unsuspecting innocent victims. The Court will hear from some of those victims through the written victim impact statements that have been submitted. These statements express the very real financial injury, not to mention the incalculable emotional distress, inflicted upon them by Ngo and his confederates.

Ultimately, as set forth in the Parties’ Joint Recommendation Regarding the Application of the United States Sentencing Guidelines, Ngo, during his three-year crime spree, caused an overwhelming guideline loss of \$65-\$100 million.

## **2. Ngo’s Role in the Criminal Conduct**

Ngo was front and center of a prolonged, multi-year assault on the financial wellbeing of hundreds of thousands, more likely millions, of U.S. citizens. Ngo devised and executed the scheme, soup to nuts. He was a jack-of-all trades: the hacker, the thief, the fraudster, the marketer, the wholesaler and the retailer of his stolen goods. He was not groomed or recruited by others. Quite the opposite. In order to expand his criminal enterprise, Ngo recruited others to

help him. For example, he found criminal “re-sellers” all over the globe and then, for a hefty sum, Ngo sold his access to PII in bulk to these re-sellers.

Ngo began engaging in the charged offenses in as early as 2010 (although he has been engaged in cyber-crime for almost 10 years) and didn’t stop until February 2013, when he was lured to, and arrested in, the U.S. During that three-year period, Ngo was responsible for (1) targeting U.S. businesses that possessed large quantities of PII, (2) hacking and defrauding his way into those businesses’ computer systems and stealing PII from them, (3) finding other hackers from whom to purchase stolen PII, (4) finding U.S. data brokers and fraudulently negotiating contracts with those brokers to buy access to their databases of PII; (5) setting up underground vending websites; (6) recruiting others to act as re-sellers; and (7) monetizing his efforts by selling the stolen data to others who, as he well knew, have used it, and unfortunately will continue to use it, to engage in fraud.

Furthermore, in order to ensure the continued “success” of his hacking and data theft operation, Ngo devised and employed sophisticated techniques to avoid detection. He had each of his criminal clients open anonymous Liberty Reserve accounts, he opened numerous e-mail accounts, one using what he believed to be a Chinese name to hide his identity, he created phony identities, he used hacked e-mail accounts, and he opened multiple overseas bank accounts with third party go-betweens.

As noted, ultimately, Ngo profited handsomely from his criminal conduct. His clients paid him \$1.75 million through Liberty Reserve accounts alone.

### **3. Ngo’s Personal Characteristics and Background**

Ngo is not, as he would have the Court believe, a naïve neophyte. Far from it. Ngo, who has an extensive background in computers, admitted during his airport confession that he has

been hacking, stealing, and re-selling payment card data and PII for the better part of a decade, dating as far back as 2007. (On the day of his arrest at the airport, Ngo provided that information in an interview conducted in Vietnamese by a Vietnamese-speaking USSS agent). Indeed, Ngo was hacking while he was a full-time college student in New Zealand. He was ultimately expelled from the university and deported from the country, ordered never to return, because of his criminal conduct. Yet Ngo continued, undeterred.

Notably, Ngo comes from a stable family with resources. He is intelligent, has highly marketable computer skills, and was in the process of getting a college degree. He had many advantages that many criminals lack. Ngo had no need to turn to a life of crime. But instead of pursuing a legitimate career and living as a law abiding citizen, Ngo consciously chose to make his life's work consist of nothing but hacking, lying, and stealing.

#### **4. Need to Protect the Public and to Provide Specific and General Deterrence**

As noted above, Ngo caused extensive harm, both financial and emotional, to a large number of innocent individuals. He caused tens of millions in financial losses and an unquantifiable amount of emotional distress. To make matters worse, Ngo was quite purposeful and calculating in his criminal conduct. Ngo's crime was not a one-time, impulsive crime. Rather, he engaged in a prolonged, methodical multi-year crime spree. Ngo was also menacing. He admitted that he thrived on being destructive, and he seemed to have an insatiable appetite for such destruction.

In stark contrast to the 3553(a) arguments advanced by Ngo's counsel in mitigation of sentence, Ngo, while testifying on November 4, 2014 as a government witness in *United States v Ealy*, 3:13-cr-175 (S.D. Ohio 2014) made the following admissions:

(1) “A. The first time I just hack for fun to enjoy myself, wreck other system, destroy something.” (United States v Ealy, 3:13-cr-175, S.D. Ohio 2014, November 4, 2014 Trial Transcript (hereafter TR) at page 2-81, lines 11-12);

(2) “A. I mean, doesn't matter which country. Yeah, it's -- if they had problems and then I can hack into their websites, I just hack to steal the credit card.” (TR at page 2-83, lines 10-12);

(3) “Q. So is a hacker generally someone who tries to break into computer systems? A. Yes. Q. How did you get involved in that? A. When I was a teenager about 16, 17 years old, and then I read on the news or newspaper. And then when I heard about hacker, I very inter-- you know, it's very interesting me. Q. Why did it interest you? A. Because they very smart, you know. And then they can wreck a system without any notice from -- from the people and without any permission. They smart, and then I want to become the same. That's why I try to research by myself through Google. Q. And when did you start getting interested in trying to be a hacker? A. About nine years ago.” (TR at page 2-71 lines 21-25 and page 2-72 lines 1-10);

(4) Q. Why would you want to hack websites for fun? A. Because I really enjoy it when I break down a system and try to find out what inside on their website or on their server. So I can use their administrator to control their website or slew something or destroy something. So it make me feel excited.” (TR at page 2-72, lines 20-25).

The transcript pages of Ngo's trial testimony in United States v Ealy referenced above are attached as Exhibit #1.

A significant prison sentence is needed here to protect the public from further harm, to mete out just punishment, and to deter Ngo and other would-be hackers. The need for deterrence is especially acute with computer hackers and other cyber-criminals like Ngo. Although quoted in the Government's initial submission, Judge Gertner's comments in United States v. Watt bear repeating:

[C]ybercrimes by their very nature allow offenders to commit the offenses without leaving their homes and with a veil of anonymity. This lack of contact with the victims of their crimes and insulation from law enforcement may cause them to be under-deterred. Only successful prosecution and significant punishment will supply prospective cyber-criminals with the information needed to create real deterrence.

707 F. Supp. 2d 149, 156-57 (D. Mass. 2010).

A 15-year sentence is needed to deter Ngo and other would-be data thieves. If cybercriminals around the world know that they can hide out safely in their home countries, remotely hack into U.S. merchants' computers, steal or fraudulently obtain access to millions of U.S. citizens' PII, cause tens of millions of dollars in losses, wreak havoc on millions of U.S. citizens, and do so with minimal punishment, then they will likely continue to engage in these crimes and injure more victims. These predators presumably already realize that it is extremely unlikely that they will be detected and criminally charged by U.S. authorities. They also undoubtedly realize that, even if they are detected and charged, it is even less likely that they will then either be lured or extradited to the U.S. If, on top of that, they learn that the punishments that are ultimately meted out to other cybercriminals who have been caught are fairly mild, then there is a serious risk that these predators will do a "cost-benefit"/"risk-reward" analysis and continue their crimes unabated. They will continue hacking into U.S. companies' computer systems, continue stealing U.S. citizens' PII, and continue wreaking havoc on businesses and individuals alike. They will instead chalk up the minimal risk of apprehension and mild punishment to the "cost of doing business," and will continue their criminal conduct, unabated and undeterred.

## **5. In Line with Other Sentences**

As noted in the Government's initial filing, a 15-year sentence in this case would also be in line with other sentences meted out in other related cases, in analogous cases in this district, and in other cases around the country. The people who bought relatively small amounts of PII from Ngo have been, and will be, sentenced to significant prison terms. Accordingly, Ngo should face an exponentially higher sentence.

## **DEFENDANT’S DEPARTURE/VARIANCE ARGUMENTS LACK MERIT**

Ngo was not the inexperienced, impressionable young man he paints himself to be in his sentencing memo. USSS Special Agent O’Neill, if he were to testify, would testify that: (1) at the time of his arrest, Ngo was the largest seller of stolen PII in the world; (2) Ngo innovatively, and exclusively, established his own web site with a user-friendly API interface that allowed his criminal clients to directly access the PII databases of U.S. companies, so that they could search for and then purchase PII of millions of U.S. citizens;<sup>3</sup> (3) Ngo was a “force multiplier” in the industry---he expanded his reign by cloning his websites and selling them to others. This in turn provided still more criminals access to the U.S. databases that Ngo had infiltrated, exponentially increasing harm to innocent victims. As a testament to Ngo’s dominance in the cybercrime underworld, SA O’Neill would add that he still receives emails from former clients of Ngo’s (sent to Ngo’s now-monitored email accounts), telling Ngo that he was the premier source of PII, anywhere, ever, and asking when Ngo will be back in business. Only this Court can prevent that from happening.

## **CONCLUSION**

### **15 Years is an Appropriate Sentence**

The recommended 15-year sentence is appropriate in light of Ngo’s anticipated USSG Sentencing Guideline’s range of 292-365 months, the Government’s 5K motion, and the 3553(a) factors described above.

---

<sup>3</sup> Attached as Exhibit #2 are three screen shots of Ngo’s web site showing: (1) the log-in screen to the web site; (2) the page on which he advertised fullz; and, (3) the redacted results of a query run by SA O’Neill using a relative’s name and the state of Virginia, which returned information on 71 people with that same name in Virginia. The first return is minimally redacted so the Court can see the types of PII Ngo’s web site made available (including SSN, DOB, address, and age) through a query of the PII database that contained over 200 million U.S. citizens’ PII, while the other 70 returns have been completely redacted. After running such a query, customers of Ngo could purchase individual pieces of PII relating to one or more individuals on the return, such as only the SSN or only the DOB, or they could buy all of the PII for any one, or any number of the people listed on the return for a particular query.

Donald Feith  
Acting United States Attorney

July 9, 2015

By: /s/ Arnold H. Huftalen  
Arnold H. Huftalen, AUSA  
Bar Association # 1215  
53 Pleasant St., 4th Floor  
Concord, NH 03301  
arnold.huftalen@usdoj.gov  
(603) 225-1552

/s/ Mona Sedky  
Mona Sedky  
Senior Trial Attorney  
U.S. Department of Justice  
Computer Crime & Intellectual Property  
Section

Certificate of Service

I certify that a copy of this Supplemental Sentencing Memorandum, with its two Exhibits, has been served upon the defendant, through counsel, via ECF Filing Notice today, July 9, 2015.

By: /s/ Arnold H. Huftalen  
Arnold H. Huftalen, AUSA